Lab 3 – Securing and lookups

1- Place confidential variables in a file **secret.yaml** :

```
secret: |
  Ceci est le message chiffré sur plusieurs lignes
  Voici la seconde ligne
```

2- Create a file containing the passwords :

```
echo "testtest" > ~/.vault_passwords.txt ;
chmod 600 ~/.vault_passwords.txt
```

3- Encrypt the secret.yaml file with the password contained in the protected area ~/.vault_passwords.txt :

```
ansible-vault encrypt secret.yml --vault-password-file ~/.vault_passwords.txt
```

You can view the contents of the secret.yaml after this command to verify that it is encrypted.

4- Write a **test-vault.yaml** playbook to display the contents of the secret variable of the **secret.yaml**

Adhoc:
> ansible-vault view --vault-id @prompt secret.yml

Playbook:

```
---
- hosts: localhost
  tasks:
   - name: Read secret file
     include_vars: "secret.yml"
   - name: display secret value
     debug:
       msg: "{{ secret }}"
```

5- Run the created playbook by specifying the vault password file :

```
ansible-playbook test-vault.yml --vault-password-file ~/.vault_passwords.txt
```

6- Use the provided csv file to display via a playbook, running on the localhost, the **web_server** user password.

```
---
- hosts: localhost
  tasks:
    - name: Read secret file
      include_vars: "secret.yml"
    - name: display secret value
      debug:
        msg: "{{ secret }}"
    - name: write the secret to a csv file
      copy: content="{{ secret }}" dest=debug.csv
```